AMENDMENTS TO THE CLAIMS

Kindly amend the claims as follows:

Claims 1 – 34 (cancelled)

35. (new) A smart card device comprising:

a controller;

a smart card reader in communication with said controller;

a communications interface coupled to said controller; and

a power source.

36. (new) The smart card device according to claim 35, configured to be connectable to any of a) a telephone and the wall socket of a telephone line, b) a cellular phone via either of a cable and another communication interface, and c) a telephone and its handset.

37. (new) The smart card device according to claim 35, wherein said communications interface includes any of a MODEM, an Ethernet interface, an infra-red (IR) interface, an RF interface, and audio tone capability.

38. (new) The smart card device according to claim 35, and further comprising any of a display screen, a numeric keypad, a function key keypad, and encryption means.

39. (new) A system for remotely verifying the identification of the user of a smart card, the system comprising:

a smart card device, comprising:

a controller;

a smart card reader in communication with said controller;

a communication network interface coupled to said controller; and

a power circuit, and

a remotely located server in communication with said communications interface comprising means for verifying the validity of the smart card being read by said smart card device and other data keyed into said device.

40. (new) The system according to claim 39, wherein said remotely located server further comprising means for performing any of validating a certificate and generating a "challenge" and accepting the "response" for said challenge.

41. (new) The system according to claim 39, wherein said other data comprises at least one of a personal identification number (PIN) and biometric data.

42. (new) The system according to claim 39, wherein said remotely located server is any of an Internet server, an Interactive Voice Recognition server (IVR), and a Point Of Sale (POS) server.

43. (new) The system according to claim 39, wherein said remotely located server further comprises means for transferring any of e-goods and e-money.

44. (new) A method for verifying the identification of the remote user of a smart card, the method comprising the steps of:

inserting a smart card into a smart card device, said smart card device comprising:

a controller;

a smart card reader in communication with said controller;

a communications interface coupled to said controller; and

a power source;

transmitting data from the smart card, via said communications interface, to a remotely located server;

inputting privately known information into said smart card device and transmitting said proof of signature to said remotely located server; and

said remotely located server verifying that said privately known information is a valid one for the card.

45. (new) The method according to claim 44, wherein said privately known information includes any of a personal identification number (PIN), biometric data, and other personally known information.

46. (new) A method for remotely purchasing goods or services, the method comprising the steps of:

inserting a smart card into a smart card device, said smart card device comprising:

a controller;

a smart card reader in communication with said controller;

a communications interface coupled to said controller; and

a power source;

selecting an item to be purchased from a supplier;

transmitting data read from the smart card, via said communications interface, to a remotely located server in communication with said supplier;

said remotely located server transferring transaction information associated with the purchase to said smart card device for approval; and

storing said transaction information in said smart card.